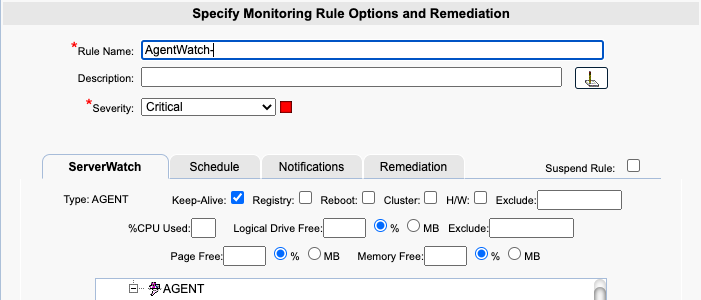
**Goliath Agent Watch Monitoring**

The Agent Watch monitoring rule allows one to monitor for settings for Windows/Linux/Unix including CPU, Memory and Disk thresholds, in addition to reboots, cluster fail over, etc, using our Goliath Intelligent Agent to alert on specified conditions.



**Configure the Monitoring**

1. To create a new monitoring condition, navigate to the **Configure - Monitoring Rules** page and click the **New** button
2. A selection pane will appear, select the radio button option for **Agent Watch** and then click **OK**
3. Now the monitoring rule pane will appear. At the top of the pane name the Monitoring Rule via the **Rule Name** field, as well as define the description and the severity.
4. The first tab, **ServerWatch** is where you will define condition(s) to be monitored.
   1. Note, only fields with values will be monitored. If you do not wish to monitor a particular metric do not enter a value in the field
5. The **Keep-Alive** checkbox, when checked, will monitor the Goliath Agents connectivity and will alert when the Goliath Agent is disconnected
6. The **Registry** checkbox, when checked, will monitor the Registry and alert when any difference is detected.
   1. For full details on how to to configure the registry settings to be alerted on see the article [Registry Monitoring](https://support.goliathtechnologies.com/hc/en-us/articles/5145194542359)
7. The **Cluster** checkbox, when checked, will monitor the cluster groups associated with the machine and will alert if there are any status or ownership changes in any of the associated Cluster Groups.
   1. For example, this will alert when the server which owns the Cluster Group switches on a fail-over to one of the other server nodes associated to the Cluster Group which then takes ownership. This would also alert if the status of the Cluster Group changes from Online to any other state such as Offline.
8. The **Reboot** checkbox, when checked, will monitor the machines uptime and will alert when the machines uptime is less than the previous check.
9. The **HW** checkbox, when checked, will monitor the machines hardware configuration and alert when any difference in Hardware Configuration is detected.
10. The **Exclude** field, next to the HW checkbox, allows one to optionally specify one or more WMI Hardware/Configuration Object names to exclude from HW/Config Check, separated by a semi-colon.
    1. For example, "Printer;CDROMDrive;NetworkAdapter" without the quotes and not case sensitive.
11. In the **%CPU Used** field, specify the percentage threshold for the Total % CPU Utilization to monitor and you will be alerted if the % CPU Utilization goes above this threshold.
12. In the **Logical Drive Free** field, specify the threshold for the Logical Drives in units of either Percent (%) or Megabytes (MB), chosen via the radio buttons next to the field in which you'd like to monitor. An alert will be triggered if the the free space drops below this threshold.
13. The **Exclude** field, next to the **Logical Drive Free** field, allows one to optionally specify one or more drives to be excluded from the drive space monitoring, separated by a semi-colon.
    1. For example, to exclude the Logical Drives D, E and F, specify as "D; E; F;" without the quotes.
14. In the **Page Free** field, specify the percentage threshold for the Virtual Memory/Page File you would like to monitor and you will be alerted if it drops below this threshold.
15. In the **Memory Free** field, specify the percentage threshold for the Physical Memory in units of either Percent (%) or Megabytes (MB), chosen via the radio buttons next to the field you would like to monitor and you will be alerted if the free space drops below this threshold.
16. In the **Selections** tree, select the machines that you want to monitor the specified condition on
    1. Please note, a machine can only be applied to one VMware Horizon View monitoring rule type at a time.

**Configure the Schedule**

The **Schedule** tab of a monitoring rule allows users to define how frequently the rule will alert. This can be done by adjusting the following fields:

* **Alert Every Time**: Defines whether an alert is generated every time the conditions are on the previous tab are met.
  + When checked the alert is generated every time the conditions are met.
  + When unchecked, the alert is only generated if the alert conditions are met, and the Minimal Notification Interval is exceeded since the last alert for this type.
* **Minimal Notification Interval**: Defines the minimal interval that must elapse between events for this alert before another alert will be generated.
  + The Alert Every Time checkbox must be unchecked in order to use this option.
  + For ServerWatch IP Services, this also defines the minimum elapsed time since a service is first detected as down or failed before an alert is generated.
* **Maximum Notification Interval**: Defines the maximum number of times you want to be notified during a continuous failure situation.
  + A value of 0 means no maximum is defined so you will continue to be notified according to your Alert Every Time and Minimal Notification Interval settings.
  + A non-zero value means that after you have been notified the number of times defined in the Maximum Alert Notifications, and according to your Alert Every Time and Minimal Notification Interval settings, you will not be notified again.
* **Notify On Restore**: Defines whether a 'Restore' alert is generated if you have previously been alerted due to a failure.
  + There is always a Notify on Restore for a ServerWatch for IP Service
* **Service Check Frequency, Every**: Defines the frequency with which the service specified for this Monitoring Rule is checked. It is no recommended to do this check any fewer then 3 mins.
* **Alert 1st Time After X Failures:**Define a value 1 or greater that defines how many successive failures should occur before the 1st alert notification 'Action' is executed.
  + The **Alert Every Time** and **Minimum Notification Interval** settings do no become applicable until after this threshold setting is exceeded.
  + The default value for this setting is blank which means not applicable. When not applicable, the **Alert Every Time** and **Minimum Notification Interval** settings are active immediately and the 1st alert does not occur until the **Minimum Notification Interval** threshold is equaled or exceeded if it is active.

**Additional Configuration**

For additional configuration options please see the following articles:

* Enabling Notifications:
  + [Configure Email and Text Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024446933)
  + [Configure SNMP Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913)
  + [Configure Syslog Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024346594)
* [Configure Custom Remediation](https://support.goliathtechnologies.com/hc/en-us/articles/360024446633)
* [Facebook](https://www.facebook.com/share.php?title=Goliath+Agent+Watch+Monitoring&u=https%3A%2F%2Fsupport.goliathtechnologies.com%2Fhc%2Fen-us%2Farticles%2F4831026126743-Goliath-Agent-Watch-Monitoring)
* [Twitter](https://twitter.com/share?lang=en&text=Goliath+Agent+Watch+Monitoring&url=https%3A%2F%2Fsupport.goliathtechnologies.com%2Fhc%2Fen-us%2Farticles%2F4831026126743-Goliath-Agent-Watch-Monitoring)